APPENDIX E TO PART 504—CUSTOMER NOTICE OF FORMAL WRITTEN REQUEST—SAMPLE FORMAT

(*Official Letterhead*)

(Date) _____

Mr./Ms. _____

1500 N. Main Street, Washington, DC 20314.

Dear Mr./Ms. ___: Information or records concerning your transactions held by the financial institution named in the attached request are being sought by the (agency/department) in accordance with the Right to Financial Privacy Act of 1978, section 3401 *et seq.*, Title 12, United States Code, and Army Regulation 190–6, for the following purpose(s):

_____

(List the purpose(s))

If you desire that such records or information not be made available, you must do the following:

a. Fill out the accompanying motion paper and sworn statement or write one of your own—

(1) Stating that you are the customer whose records are being requested by the Government.

(2) Giving the reasons you believe that the records are not relevant or any other legal basis for objecting to the release of the records.

b. File the motion and statement by mailing or delivering them to the clerk of any one of the following United States District Courts:

_____

(List applicable courts)

c. Mail or deliver a copy of your motion and statement to the requesting authority: (give title and address).

d. Be prepared to come to court and present your position in further detail.

You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of (10 days from the date of personal service) (14 days from the date of mailing) of this notice, the records or information requested therein may be made available.

These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer if such transfer is made.

3 Enclosures (see para ___)

(Signature) _____

PART 505—ARMY PRIVACY ACT PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 71 FR 46052, Aug. 10, 2006, unless otherwise noted.

§ 505.1 General information.

(a) *Purpose.* This part sets forth policies and procedures that govern personal information maintained by the Department of the Army (DA) in Privacy Act systems of records. This part also provides guidance on collecting and disseminating personal information in general. The purpose of the Army Privacy Act Program is to balance the government's need to maintain information about individuals with the right of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance,

use and disclosure of personal information about them. Additionally, this part promotes uniformity within the Army's Privacy Act Program.

(b) *References:* (1) Referenced publications are listed in Appendix A of this part.

(2) DOD Computer Matching Program and other Defense Privacy Guidelines may be accessed at the Defense Privacy Office Web site *http://www.defenselink.mil/privacy*.

(c) Definitions are provided at Appendix H of this part.

(d) *Responsibilities.* (1) The Office of the Administrative Assistant to the Secretary of the Army will—

(i) Act as the senior Army Privacy Official with overall responsibility for the execution of the Department of the Army Privacy Act Program;

(ii) Develop and issue policy guidance for the program in consultation with the Army General Counsel; and

(iii) Ensure the DA Privacy Act Program complies with Federal statutes, Executive Orders, Office of Management and Budget guidelines, and 32 CFR part 310.

(2) The Chief Attorney, Office of the Administrative Assistant to the Secretary of the Army (OAASA) will—

(i) Provide advice and assistance on legal matters arising out of, or incident to, the administration of the DA Privacy Act Program;

(ii) Serve as the legal advisor to the DA Privacy Act Review Board. This duty may be fulfilled by a designee in the Chief Attorney and Legal Services Directorate, OAASA;

(iii) Provide legal advice relating to interpretation and application of the Privacy Act of 1974; and

(iv) Serve as a member on the Defense Privacy Board Legal Committee. This duty may be fulfilled by a designee in the Chief Attorney and Legal Services Directorate, OAASA.

(3) The Judge Advocate General will serve as the Denial Authority on requests made pursuant to the Privacy Act of 1974 for access to or amendment of Army records, regardless of functional category, concerning actual or potential litigation in which the United States has an interest.

(4) The Chief, DA Freedom of Information Act and Privacy Office (FOIA/P), U.S. Army Records Management and Declassification Agency will—

(i) Develop and recommend policy;

(ii) Execute duties as the Army's Privacy Act Officer;

(iii) Promote Privacy Act awareness throughout the DA;

(iv) Serve as a voting member on the Defense Data Integrity Board and the Defense Privacy Board;

(v) Represent the Department of the Army in DOD policy meetings; and

(vi) Appoint a Privacy Act Manager who will—

(A) Administer procedures outlined in this part;

(B) Review and approve proposed new, altered, or amended Privacy Act systems of records notices and subsequently submit them to the Defense Privacy Office for coordination;

(C) Review Department of the Army Forms for compliance with the Privacy Act and this part;

(D) Ensure that reports required by the Privacy Act are provided upon request from the Defense Privacy Office;

(E) Review Computer Matching Agreements and recommend approval or denial to the Chief, DA FOIA/P Office;

(F) Provide Privacy Act training;

(G) Provide privacy guidance and assistance to DA activities and combatant commands where the Army is the Executive Agent;

(H) Ensure information collections are developed in compliance with the Privacy Act provisions;

(I) Ensure Office of Management and Budget reporting requirements, guidance, and policy are accomplished; and

(J) Immediately review privacy violations of personnel to locate the problem and develop a means to prevent recurrence of the problem.

(5) Heads of Department of the Army activities, field-operating agencies, direct reporting units, Major Army commands, subordinate commands down to the battalion level, and installations will—

(i) Supervise and execute the privacy program in functional areas and activities under their responsibility; and

(ii) Appoint a Privacy Act Official who will—

(A) Serve as the staff advisor on privacy matters;

(B) Ensure that Privacy Act records collected and maintained within the Command or agency are properly described in a Privacy Act system of records notice published in the FEDERAL REGISTER;

(C) Ensure no undeclared systems of records are being maintained;

(D) Ensure Privacy Act requests are processed promptly and responsively;

(E) Ensure a Privacy Act Statement is provided to individuals when information is collected that will be maintained in a Privacy Act system of records, regardless of the medium used to collect the personal information (*i.e.*, forms, personal interviews, stylized formats, telephonic interviews, or other methods);

(F) Review, biennially, recordkeeping practices to ensure compliance with the Act, paying particular attention to the maintenance of automated records. In addition, ensure cooperation with records management officials on such matters as maintenance and disposal procedures, statutory requirements, forms, and reports; and

(G) Review, biennially Privacy Act training practices. This is to ensure all personnel are familiar with the requirements of the Act.

(6) DA Privacy Act System Managers and Developers will—

(i) Ensure that appropriate procedures and safeguards are developed, implemented, and maintained to protect an individual's personal information;

(ii) Ensure that all personnel are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act Program;

(iii) Ensure official filing systems that retrieve records by name or other personal identifier and are maintained in a Privacy Act system of records have been published in the FEDERAL REGISTER as a Privacy Act system of records notice. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by 5 U.S.C. 552a, as amended, OMB Circular A–130, 32 CFR part 310 and this part, will be subject to possible criminal penalties and/or administrative sanctions;

(iv) Prepare new, amended, or altered Privacy Act system of records notices and submit them to the DA Freedom of Information and Privacy Office for review. After appropriate coordination, the system of records notices will be submitted to the Defense Privacy Office for their review and coordination;

(v) Review, biennially, each Privacy Act system of records notice under their purview to ensure that it accurately describes the system of records;

(vi) Review, every four years, the routine use disclosures associated with each Privacy Act system of records notice in order to determine if such routine use continues to be compatible with the purpose for which the activity collected the information;

(vii) Review, every four years, each Privacy Act system of records notice for which the Secretary of the Army has promulgated exemption rules pursuant to Sections (j) or (k) of the Act. This is to ensure such exemptions are still appropriate;

(viii) Review, every year, contracts that provide for the maintenance of a Privacy Act system of records to accomplish an activity's mission. This requirement is to ensure each contract contains provisions that bind the contractor, and its employees, to the requirements of 5 U.S.C. 552a(m)(1); and

(ix) Review, if applicable, ongoing Computer Matching Agreements. The Defense Data Integrity Board approves Computer Matching Agreements for 18 months, with an option to renew for an additional year. This additional review will ensure that the requirements of the Privacy Act, Office of Management and Budget guidance, local regulations, and the requirements contained in the Matching Agreements themselves have been met.

(7) All DA personnel will—

(i) Take appropriate actions to ensure personal information contained in a Privacy Act system of records is protected so that the security and confidentiality of the information is preserved;

(ii) Not disclose any personal information contained in a Privacy Act system of records except as authorized by 5 U.S.C. 552a, DOD 5400.11–R, or other applicable laws. Personnel willfully making a prohibited disclosure are subject to possible criminal penalties and/or administrative sanctions; and

(iii) Report any unauthorized disclosures or unauthorized maintenance of new Privacy Act systems of records to the applicable activity's Privacy Act Official.

(8) Heads of Joint Service agencies or commands for which the Army is the Executive Agent or the Army otherwise provides fiscal, logistical, or administrative support, will adhere to the policies and procedures in this part.

(9) Commander, Army and Air Force Exchange Service, will supervise and execute the Privacy Program within that command pursuant to this part.

(10) Overall Government-wide responsibility for implementation of the Privacy Act is the Office of Management and Budget. The Department of Defense is responsible for implementation of the Act within the armed services. The Privacy Act also assigns specific Government-wide responsibilities to the Office of Personnel Management and the General Services Administration.

(11) Government-wide Privacy Act systems of records notices are available at *http://www.defenselink.mil/privacy*.

(e) *Legal Authority*. (1) Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974.

(2) Title 5, United States Code, Section 552, The Freedom of Information Act (FOIA).

(3) Office of Personnel Management, Federal Personnel Manual (5 CFR parts 293, 294, 297, and 7351).

(4) OMB Circular No. A–130, Management of Federal Information Resources, Revised, August 2003.

(5) DOD Directive 5400.11, Department of Defense Privacy Program, November 16, 2004.

(6) DOD Regulation 5400.11–R, Department of Defense Privacy Program, August 1983.

(7) Title 10, United States Code, Section 3013, Secretary of the Army.

(8) Executive Order No. 9397, Numbering System for Federal Accounts Relating to Individual Persons, November 30, 1943.

(9) Public Law 100–503, the Computer Matching and Privacy Act of 1974.

(10) Public Law 107–347, Section 208, Electronic Government (E-Gov) Act of 2002.

(11) DOD Regulation 6025.18–R, DOD Health Information Privacy Regulation, January 24, 2003.

§ 505.2 General provisions.

(a) *Individual privacy rights policy*. Army policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with the Privacy Act are as follows—

(1) Protect the privacy of United States living citizens and aliens lawfully admitted for permanent residence from unwarranted intrusion.

(2) Deceased individuals do not have Privacy Act rights, nor do executors or next-of-kin in general. However, immediate family members may have limited privacy rights in the manner of death details and funeral arrangements of the deceased individual. Family members often use the deceased individual's Social Security Number (SSN) for federal entitlements; appropriate safeguards must be implemented to protect the deceased individual's SSN from release. Also, the Health Insurance Portability and Accountability Act extends protection to certain medical information contained in a deceased individual's medical records.

(3) Personally identifiable health information of individuals, both living and deceased, shall not be used or disclosed except for specifically permitted purposes.

(4) Maintain only such information about an individual that is necessary to accomplish the Army's mission.

(5) Maintain only personal information that is timely, accurate, complete, and relevant to the collection purpose.

(6) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

(7) Maintain records for the minimum time required in accordance with an approved National Archives and Records Administration record disposition.

(8) Let individuals know what Privacy Act records the Army maintains by publishing Privacy Act system of records notices in the FEDERAL REGISTER. This will enable individuals to review and make copies of these